LISTING OF CLAIMS

1. (Currently amended) A secure messaging system comprising:

a personal record comprising a personal profile about a subject and a message filtering policy determined by the subject;

an anonymity service, the anonymity service being an intermediary between the subject and a message sponsor, the message sponsor desiring to send a message to the subject based on the personal record;

a message deposit sent to the anonymity service by the message sponsor wherein the message deposit comprises the message, a message targeting specification, and a message profile;

a database maintained by the anonymity service, the personal record being stored in the database in an encrypted state, the anonymity service having an access to the personal record only in the encrypted state;

a resident application residing on a client device under control of the subject, the resident application managing access to the personal record in an unencrypted state by use of a security element including an encrypted private key;

a quarantine memory, the quarantine memory being a secure area of system memory on the client device; and

a session agent configured to perform a database operation on the personal record in the unencrypted state in the quarantine memory,

wherein the resident application, the quarantine memory and the session agent all reside on the client device under control of the subject, and

wherein the resident application, the quarantine memory and the session agent collectively secure the personal record and the private key in an unencrypted state against access by the anonymity service.

2. (Original) The system of claim 1 wherein the database operation comprises:

a database query which compares the message profile to the message filtering policy; and

a database query which compares the personal profile to the message targeting specification.

3. (Original) The system of claim 1 further comprising:

a query result sent to the anonymity service from the resident application;

a message delivery sent from the anonymity service to the resident application; and

a delivery confirmation sent from the resident application to the anonymity service.

4. (Original) The system of claim 1 wherein the database operation comprises a data record modification.

5. (Original) The system of claim 1 wherein the database operation comprises a schema migration.

6. (Original) The system of claim 1 further comprising a delivery notification sent from the anonymity service to the sponsor wherein the delivery notification comprises:

an anonymous proof of delivery;

an anonymous response from the subject; and

an anonymous payment record.

7. (Previously presented) The system of claim 2 further comprising an interactive response from the subject.

8. (Currently amended) A secure messaging method comprising:

maintaining a personal record belonging to a subject in a centralized database in an encrypted form, the personal record comprising a personal profile and a message filtering policy; and

distributing a database operation from the centralized database to a client device, ~~when~~ wherein the database operation is performed on the personal record in an unencrypted form in a quarantine memory at the client device by use of a security element including an encrypted private key securely maintained by and accessible only to the subject such that the encrypted private key is inaccessible to the anonymity service.

9. (Currently amended) The method of claim 8 wherein distributing the database operation from the centralized database to the client device comprises:

downloading a session agent by a resident application, the resident application being resident on the client device, the session agent comprising a software update, the personal record, and the security element including [an encryption] the encrypted private key; and

performing a database query by the session agent on the personal record in an unencrypted form.

10. (Original) The method of claim 8 wherein the client device comprises a device capable of sending and receiving a signal over a digital network, the client device being under a physical control of the subject.

11. (Original) The method of claim 8 further comprising establishing an intermediary between the subject and a message sponsor for the purpose of allowing the message sponsor to send a message to the subject based on the personal profile while maintaining an anonymity of the subject.

12. (Currently amended) The method of claim 11 wherein establishing the intermediary between the subject and the message sponsor comprises:

receiving a message deposit from the message sponsor, the message deposit comprising a message, a message targeting specification, and a message profile;

negotiating permission to deliver the message to the subject;

delivering the message to the subject;

receiving a delivery confirmation from the subject; and

sending the delivery confirmation to the message sponsor while maintaining an anonymity of the subject.

13. (Original) The method of claim 12 wherein negotiating permission to deliver the message comprises:

performing a targeting database query wherein the message targeting specification is compared to the personal profile; and

performing a filtering database query wherein the message filtering policy is compared to the message profile.

14. (Original) The method of claim 12 further comprising:

accounting for a message charge to the message sponsor;

accounting for a message credit to the subject;

communicating the message charge to an external payment system; and

communicating the message credit to an external payment system.

15. (Currently amended) A machine-executable medium comprising instructions that, when executed by a machine, cause the machine to:

maintain a personal record belonging to a subject in a centralized database in an encrypted form, the personal record comprising a personal profile and a message filtering policy; and

distribute a database operation from the centralized database to a client device, ~~when~~ wherein the database operation is performed on the personal record in an unencrypted form in a quarantine memory at the client device by use of a security element including an encrypted private key securely maintained by and accessible only to the subject such that the encrypted private key is inaccessible to all others.

16. (Currently amended) The machine-executable medium of claim 15 wherein causing the machine to distribute the database operation from the centralized database to the client device comprises causing the machine to:

download a session agent by a resident application, the resident application being resident on the client device, the session agent comprising a software update, the personal record, and the security element including [an encryption] the encrypted private key; and

perform a database query by the session agent on the personal record in an unencrypted form.

17. (Previously Presented) The machine-executable medium of claim 15 wherein the client device comprises:

a device capable of sending and receiving a signal over a digital network, the client device being under a physical control of the subject.

18. (Previously Presented) The machine-executable medium of claim 15 further comprising instructions that, when executed by a machine, cause the machine to establish an intermediary between the subject and a message sponsor for the purpose of allowing the message sponsor to send a message to the subject based on the personal profile while maintaining an anonymity of the subject.

19. (Currently amended) The machine-executable medium of claim 18 wherein causing the machine to establish the intermediary between the subject and the message sponsor comprises causing the machine to:

receive a message deposit from the message sponsor, the message deposit comprising a message, a message targeting specification, and a message profile;

negotiate permission to deliver the message to the subject;

deliver the message to the subject;

receive a delivery confirmation from the subject; and

send the delivery confirmation to the message sponsor while maintaining an anonymity of the subject.

20. (Previously Presented) The machine-executable medium of claim 19 wherein causing the machine to negotiate permission to deliver the message comprises causing the machine to:

perform a targeting database query wherein the message targeting specification is compared to the personal profile; and

perform a filtering database query wherein the message filtering policy is compared to the message profile.

21. (Previously Presented) The machine-executable medium of claim 19 further comprising causing the machine to:

account for a message charge to the message sponsor;

account for a message credit to the subject;

communicate the message charge to an external payment system; and

communicate the message credit to an external payment system.

22. (Previously Presented) The system of claim 1 wherein the quarantine memory at least temporarily contains the personal record in an unencrypted state and a private key also in an unencrypted state.

23. (Currently amended) The system of claim [[23]] 22, wherein the quarantine memory contents including the personal record and the private key are deleted at an end of a client session.